Notice of Allowability	Application No.	Applicant(s)	
	09/705,998	JUTLA, CHARANJIT SINGH	
	Examiner	Art Unit	
	Jacob F. Betit	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *applicant's amendment filled 13 October 2004* .

2. ☒ The allowed claim(s) is/are *1-47*.

3. ☒ The drawings filed on *21 May 2004* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20050218* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

C. Rones

CHARLES RONES
PRIMARY EXAMINER

DETAILED ACTION

Remarks

1. In response to communications filed on 13-October-2004, claims 1-47 are presently pending in the application.

2. In view of the examiner's amendment, authorized by Attorney of Record, claims 1-47 are amended by the examiner (details provided below).

Examiner's Amendment

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Dr. Louis P. Herzberg on 17-February-2005 (see enclosed Interview Summary for details).

The application has been amended as follows. This listing of claims will replace all prior versions of the claims in the application.

1. (Original) A method for encrypting a plain-text message, the method comprising:

generating a first random number;

transforming said first random number into a first pseudo random number;

further expanding a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

dividing said plain-text message into a plurality of plain-text blocks;

encrypting said plain-text blocks to form a plurality of cipher-text blocks;

combining said plurality of plain-text blocks into at least one check sum; and

employing said set of pair-wise differentially-uniform pseudo random numbers, together with said first random number and/or said first pseudo random number, to embed a message integrity check in said cipher-text blocks.

2. (Previously presented) A method as recited in claim 1, wherein the step of encrypting said plain-text blocks includes employing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers.

3. (Original) A method as recited in claim 1, wherein the step of employing includes pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks; and

combining each pair to form a plurality of output blocks.

4. (Original) A method as recited in claim 3, wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair.

5. (Original) A method as recited in claim 1, wherein the step of encrypting includes encrypting said first random number.

6. (Original) A method as recited in claim 1, wherein the step of encrypting includes encrypting said check sum.

7. (Original) A method as recited in claim 1, wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks.

8. (Original) A method as recited in Claim 1, wherein the step of transforming said random number includes a non-cryptographic or linear operation.

9. (Original) A method as recited in Claim 1, wherein the step of transforming said random number includes a cryptographic operation.

10. (Previously presented) A method as recited in Claim 1, wherein said set of pair-wise differentially-uniform numbers are set of pair-wise differentially-uniform numbers in GFp.

11. (Original) A method as recited in claim 2, wherein the step of employing includes:

pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of plain-text blocks; and

combining each pair to form a plurality of input blocks used in said step of encrypting.

12. (Original) A method as recited in claim 11, wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair.

13. (Currently amended) A method for decrypting a cipher-text message, the method comprising:

dividing said cipher-text message into a plurality of cipher-text blocks;

decrypting said cipher-text blocks in forming a plurality of plain-text blocks;

transforming at least one of said plain-text blocks into a first pseudo random number;

further expanding at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

combining ~~said first pseudo random number, and/or~~ said set of pair-wise differentially-uniform pseudo random numbers, and said first pseudo random number and/or said at least one plain-text block to form at least two check sums and to form a plurality of output blocks; and

comparing said at least two check sums in declaring success of a message integrity check.

14. (Original) A method as recited in claim 13, wherein the step of decrypting said cipher-text blocks includes employing said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers.

15. (Original) A method as recited in claim 13, wherein the step of combining includes:

pairing said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of plain-text blocks; and

using each pair to form a plurality of output blocks and employing the output blocks to form said at least two check sums.

16. (Original) A method as recited in claim 15, wherein the step of using each pair includes performing an exclusive-or operation upon components of said each pair.

17. (Previously presented) A method as recited in claim 15, wherein the step of forming includes:

dividing said output blocks into at least two subsets, and

obtaining said at least two checksums from an exclusive-or of said subsets of output blocks.

18. (Original) A method as recited in Claim 13, wherein the step of transforming said plain-text blocks includes a non-cryptographic or linear operation.

19. (Original) A method as recited in Claim 13, wherein the step of transforming said plain-text blocks includes a cryptographic operation.

20. (Previously presented) A method as recited in Claim 13, wherein said set of pair-wise differentially-uniform numbers are set of pair-wise differentially-uniform numbers in GFp.

21. (Original) A method as recited in claim 14, wherein the step of employing includes:

pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks; and

combining each pair to form a plurality of input blocks used in said step of decrypting.

22. (Original) A method as recited in claim 3, wherein p is a prime number, and the step of combining each pair includes performing a modulo p addition upon components of said each pair.

23. (Original) A method as recited in claim 11, wherein p is a prime number, and the step of combining each pair includes performing a modulo p addition upon components of said each pair.

24. (Original) A method as recited in claim 15, wherein p is a prime number, and the step of using each pair includes performing a modulo p addition upon components of said each pair.

25. (Original) A method as recited in claim 21, wherein p is a prime number, and the step of combining each pair includes performing a modulo p addition upon components of said each pair.

26. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

27. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a cipher-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 13.

28. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 1.

29. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a plain-text message, the computer readable program code means in said computer program product

comprising computer readable program code means for causing a computer to effect the steps of claim 13.

30. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 1.

31. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for decrypting a cipher-text message, said method steps comprising the steps of claim 13.

32. (Previously presented) A method for encryption/decryption of a plain-text message, the method comprising the steps of:

generating a first random number;

transforming said first random number into a first pseudo random number;

further expanding a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

dividing the plain-text message into a plurality of plain-text blocks;

encrypting said plain-text blocks in forming a plurality of cipher-text blocks;

combining said plurality of plain-text blocks into at least one check sum; and

employing said first random number, said first pseudo random number and said set of pair-wise differentially-uniform pseudo random numbers to embed a message integrity check in said cipher-text blocks to form a cipher-text message; and

dividing said cipher-text message into a plurality of cipher-text blocks;

decrypting said cipher-text blocks in forming a plurality of plain-text blocks;

transforming at least one of said plain-text blocks into a first pseudo random number;

further expanding at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

combining said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, and/or said at least one plain-text block to form at least two check sums and to re-form the said plain-text message; and

comparing said at least two check sums in declaring success of a message integrity check in decryption of said cipher-text to reform said plain-text message.

33. (Original) An apparatus to encrypt a plain-text message, the apparatus comprising:

a Randomness Generator to generate a first random number;

a Randomness Transformer to transform said first random number into a first pseudo random number;

a Pairwise Additively Uniform Sequence Generator to further expand a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

an Encryptor to divide said plain-text message into a plurality of plain-text blocks, and to encrypt said plain-text blocks to form a plurality of cipher-text blocks;

a Checksum Generator to combine said plurality of plain-text blocks into at least one check sum; and

an Integrity Extractor and Checker to employ said set of pair-wise differentially-uniform pseudo random numbers, together with said first random number and/or said first pseudo random number, to embed a message integrity check in said cipher-text blocks.

34. (Currently amended) An apparatus to decrypt a cipher-text message, the apparatus comprising:

a Decryptor to divide said cipher-text message into a plurality of cipher-text blocks, and to decrypt said cipher-text blocks in forming a plurality of plain-text blocks;

a Randomness Transformer to transform at least one of said plain-text blocks into a first pseudo random number;

a Pairwise Additively Uniform Sequence Generator to further expand at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

a Checksum Generator to combine ~~said first pseudo random number, and/or~~ said set of pair-wise differentially-uniform pseudo random numbers, and said first pseudo random number, and/or said at least one plain-text block to form at least two check sums and to form a plurality of output blocks; and

an Integrity Extractor and Checker to compare said at least two check sums in declaring success of a message integrity check.

35. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 2.

36. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a cipher-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 14.

37. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 2.

38. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 14.

39. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 2.

40. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for decrypting a cipher-text message, said method steps comprising the steps of claim 14.

41. (Original) A method as recited in claim 3, wherein the step of combining each pair includes performing an addition in a group upon components of said each pair.

42.(Previously presented) A method as recited in claim 11, wherein the step of combining each pair includes performing an addition in a group upon components of said each pair.

43. (Original) A method as recited in claim 15, wherein the step of using each pair includes performing an addition in a group upon components of said each pair.

44. (Original) A method as recited in claim 21, wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair.

45. (Original) A method as recited in claim 21, wherein the step of combining each pair includes performing an addition in a group upon components of said each pair.

46. (Previously presented) A method as recited in Claim 33, wherein at least one element performs a plurality of operations in parallel.

47. (Previously presented) A method as recited in Claim 1, wherein the step of encrypting said plain-text blocks is performed in parallel for a plurality of said plain-text blocks.

Allowance

4. The following is an examiner's statement of reasons for allowance:

The prior art of record does not disclose, teach, or suggest the claimed limitations of (in combination with all other features in the claim):

Employing said set of pair-wise differentially-uniform pseudo random numbers, together with said first random number and/or said first pseudo random number, to embed a message integrity check in said cipher text blocks as claimed in claim 1.

The prior art of record does not disclose, teach, or suggest the claimed limitations of (in combination with all the other features of the claim):

Combining said set of pair-wise differentially-uniform pseudo random numbers, and said first pseudo random number and/or said at least one plain-text block to form at least two check sums and to form a plurality of output blocks as claimed in claim 13.

The prior art of record does not disclose, teach, or suggest the claimed limitations of (in combination with all the other features of the claim):

Employing said first random number, said first pseudo random number and said set of pair-wise differentially-uniform random numbers to embed a message integrity check in said cipher-text blocks to form a cipher text message as claimed in claim 32.

The prior art of record does not disclose, teach, or suggest the claimed limitations of (in combination with all the other features of the claim):

An Integrity Extractor and Checker to employ said set of pair-wise differentially uniform pseudo random numbers, together with said first random number and/or said first pseudo random number, to embed a message integrity check in said cipher-text blocks as claimed in claim 33.

The prior art of record does not disclose, teach, or suggest the claimed limitations of (in combination with all the other features of the claim):

A Checksum Generator to combine said set of pair-wise differentially-uniform pseudo random numbers, and said first pseudo random number, and/or said at least one plain-text block to form at least two check sums and to form a plurality of output blocks as claimed in claim 34.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (571) 272-4075. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (571) 272-4083. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jfb
18 Feb 2005

C. Rones
CHARLES RONES
PRIMARY EXAMINER